UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/537,517	06/03/2005	Markus Feuser	DE02 0290 US	3562

65913 7590 04/08/2009

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/08/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/537,517	FEUSER ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 February 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 6-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 6-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5 February 2009 has been entered. In this amendment, claims 1, 2, 6, 7, 9, and 10 have been amended, and claims 13-16 have been added.

2. Claims 1-4 and 6-16 are presented for examination.

Response to Arguments

3. With regards to the objection to the specification, the applicant has submitted amendments, and the examiner hereby withdraws the objection.

4. Applicant's arguments with respect to claims 1-12 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 4, 6, 10, and 14-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Rose et al. (US 2004/0039908 A1 and Rose hereinafter).

As to claim 1, Rose discloses a system and method for encrypting and authenticating data (0010, lines 1-4), the system and method having:

at least two access-secured sub-areas (i.e. plaintext blocks)**, each having at least one assigned part** (i.e. bits) **of a parameter** (i.e. partial block) **comprising at least one bit, the device configured such that an encryption method is applied to fewer than all of said sub-areas** (0010, lines 8-14);

an encryption block, wherein said encryption block receives at least one assigned part of said parameter from at least one of said sub-areas (i.e. plaintext blocks) **and encrypts said part of said parameter** (i.e. partial block) (0010, lines 13-14).

As to claim 6, Rose discloses:

receiving a parameter, by a data processing device, wherein the parameter is comprised of at least two parts, each part comprising at least one bit (0006, lines 8-16; 0084, lines 2-6; 0092, lines 1-4);

assigning, by said data processing device, said parts of the parameter into at least two access-secured sub-areas (i.e. plaintext blocks)

located in said data-processing device (0006, lines 8-16; 0010, lines 4-6; 0084, lines 2-6).

encrypting, by said data processing device, at least one of said parts of the parameter (i.e. partial block) **in said access-secured sub-areas** (i.e. plaintext block) **with an encryption method, wherein said encryption method is applied to fewer than all of said sub-areas** (0006, lines 8-16; 0010, lines 8-14).

As to claim 10, Rose discloses:

at least two access-secured sub-areas (i.e. plaintext block)**, each having at least one assigned part of a parameter** (i.e. partial block) **comprising at least one bit, the device configured such that an encryption method is applied to fewer than all of said sub-areas** (0010, lines 8-14)**, the data processing device utilized in at least one of: a one smart card controller, a reader integrated circuit, a cryptography chipset, or for application in at least one of audio or video encryption** (0026, lines 8-15).

As to claim 4, Rose discloses:

wherein the memory component comprises an erasable programmable read only memory, an electrically erasable programmable read only memory or a flash memory (0112, lines 5-7).

As to claims 14-16, Rose discloses:

wherein said device encrypts at least one part of said parameter (i.e. partial block)**, but not all parts of said parameter** (0084, lines 2-6).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2, 3, 7, and 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rose as applied to claims 1, 6, and 10 above, and in view of Candelore et al. (EP 0908810 A2 and Candelore hereinafter).

As to claims 2 and 7, Rose fails to specifically disclose:

> **wherein the encrypted part of the parameter in a first of the at least two access-secured sub-areas is encrypted as a function of at least one part of the parameter of a second of the at least two sub-areas.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rose, as taught by Candelore.

Candelore discloses a system and method for block chaining and block re-ordering (Abstract, lines 1-4), the system and method having:

> **wherein the encrypted part of the parameter in a first of the at least two access-secured sub-areas** (i.e. block) **is encrypted** (i.e. keyed/hashed) **as a function of at least one part of the parameter of a second** (i.e. block 2) **of the at least two sub-areas** (col. 24, lines 12-15; col. 25, lines 12-18)**.**

Given the teaching of Candelore, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rose with the teachings of Candelore by performing encryption based on information of another sub-area. Candelore recites motivation by disclosing that if any of the program information of a block is changed, the decrypted output would change, causing the authentication verification to fail (col. 17, lines 43-47). Candelore also discloses that cipher block chaining is a robust encryption algorithm because a change in one block will cascade changes to other blocks making it difficult for a pirate to effect a simple change to the program information (col. 14, lines 29-32). It is obvious that the teachings of Candelore would have improved the teachings of Rose by performing encryption based on a parameter of another sub-area in order to provide for robust encryption that prevents a change in one area from being authenticated.

As to claim 3, Rose fails to specifically disclose:

> **wherein at least one of the input value to the function or the return value from the function is more than one bit wide.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rose, as taught by Candelore.

Candelore discloses:

> **wherein at least one of the input value to the function or the return value from the function is more than one bit wide** (col. 21, lines 39-41).

Given the teaching of Candelore, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rose with the teachings of Candelore by having an input or output that is more than one bit. Candelore recites motivation by disclosing that using blocks of data in chaining is efficient due to the relatively low overhead of the authentication information relative to the authenticated data (col. 21, lines 41-43). It is obvious that the teachings of Candelore would have improved the teachings of Rose by using an input/output that is larger than one bit in order to increase efficiency.

As to claims 11-13, Rose fails to specifically disclose:

wherein the at least one assigned parameter comprises an address.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rose, as taught by Candelore.

Candelore discloses:

wherein the at least one assigned parameter comprises an address

(col. 24, lines 15-17).

Given the teaching of Candelore, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rose with the teachings of Candelore by using an address as the parameter. Candelore recites motivation by disclosing that using the address provides for authentication that is dependent on a location (col. 24, lines 15-17). Candelore also discloses that when the key used for each block of a chain is dependent

on an address, each key would be different (col. 17, lines 41-43). It is obvious that the teachings of Candelore would have improved the teachings of Rose by using an address is a parameter in order to provide for authentication that is dependent on a location of data.

9. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rose in view of Candelore as applied to claim 7 above, and further in view of Toh et al. (US 2002/0048372 A1 and Toh hereinafter).

As to claim 8, Rose in view of Candelore fails to specifically disclose:

characterized in that the function is one-to-one.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rose in view of Candelore, as taught by Toh. Toh discloses a system and method for generating and utilizing a universal signature object for digital data (0017, lines 1-3), the system and method having:

characterized in that the function is one-to-one (0012, lines 16-18).

Given the teaching of Toh, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rose in view of Candelore with the teachings of Toh by using a one-to-one function. Toh recites motivation by disclosing that using a one-to-one hash function allows for each hash number to generate one data file so that changes in the data can be detected (0012, lines 17-20). It is obvious that the teachings of Toh would have

improved the teachings of Rose in view of Candelore by using a one-to-one function for encryption in order to be able to detect changes in the data.

10. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rose as applied to claim 6 above, and in view of Unger et al. (US 2003/0026423 A1 and Unger hereinafter).

As to claim 9, Rose fails to specifically disclose:

wherein each access-secured sub-area is encrypted with a separate encryption method.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Rose, as taught by Unger.

Unger discloses a system and method for multiple encrypting only a portion of the data required for full presentation of a television program (Abstract, lines 1-4), the system and method having:

wherein each access-secured sub-area is encrypted with a separate encryption method (0103, lines 4-7).

Given the teaching of Unger, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Rose with the teachings of Unger by encrypting each sub-area with a separate encryption method. Unger recites motivation by disclosing that duplicating each encrypted program for each type of encryption allows each form to be provided simultaneously, allowing for a provider to change or upgrade a chosen encryption

scheme without requiring multiple mode capability in set-top boxes (0007, lines 1-8; 0008, lines 1-7). It is obvious that the teachings of Unger would have improved the teachings of Rose by encrypting each sub-area with a separate encryption method in order to prevent the increase in cost of multiple mode set-top boxes while allowing a cable operator to update its chosen encryption scheme.

Prior Art Made of Record

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Fetkovich et al. (US Patent 7,151,832 B1) discloses a system and method for dynamic encryption and decryption of a stream of data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431